Notes

THE DATA BREACH DILEMMA: PROACTIVE SOLUTIONS FOR PROTECTING CONSUMERS' PERSONAL INFORMATION

DANIEL J. MARCUS†

ABSTRACT

Data breaches are an increasingly common part of consumers' lives. No institution is immune to the possibility of an attack. Each breach inevitably risks the release of consumers' personally identifiable information and the strong possibility of identity theft.

Unfortunately, current solutions for handling these incidents are woefully inadequate. Private litigation like consumer class actions and shareholder lawsuits each face substantive legal and procedural barriers. States have their own data security and breach notification laws, but there is currently no unifying piece of legislation or strong enforcement mechanism.

This Note argues that proactive solutions are required. First, a national data security law—setting minimum data security standards, regulating the use and storage of personal information, and expanding the enforcement role of the Federal Trade Commission—is imperative to protect consumers' data. Second, a proactive solution requires reconsidering how to minimize the problem by going to its source: the collection of personally identifiable information in the first place. This Note suggests regulating companies' collection of Social Security numbers, and, eventually, using a system based on distributed ledger technology to replace the ubiquity of Social Security numbers.

† Duke University School of Law, J.D. expected 2019; Cornell University, B.A. 2014. My thanks to Governor Sarah Bloom Raskin for inspiring me to write about the growing issues in cybersecurity and always serving as a sounding board. This Note would not be possible without the guidance and helpful feedback from Professors Emily Strauss and Shane Stansbury, as well as the participants in the Scholarly Writing Workshop. Also, many thanks to the editors of the *Duke Law Journal* for their hard work in helping refine my piece, and of course, to Samantha and my family for their love and support.

INTRODUCTION

There is a high probability that your financial and personal information—name, address, Social Security number, birth date, and more—has been stolen. On September 7, 2017, the credit reporting agency Equifax[1] announced that its database had been hacked, potentially compromising sensitive information of approximately 143 million American consumers[2]—meaning that the breach affected about 44 percent of the population.[3] Four months prior to Equifax's announcement, hackers exploited a bug in the company's software and gained access to its entire internal system.[4] While a patch was available in March 2017, former Equifax CEO Richard Smith blamed a single individual for failing to take any action to patch the bug.[5] Additionally, a routine scan of the security system failed to detect the vulnerability.[6] This left Equifax's entire centralized database of financial and personal information wide-open to an attack.

The Equifax breach has drawn heightened attention to the prevalence of data breaches and the security issues that inevitably follow. Recent data breaches of companies like Facebook, Target, Home Depot, Yahoo, and even the U.S. Office of Personnel Management, have exposed millions of individuals' sensitive personal information.[7] However, unlike Facebook or Yahoo users, consumers

1. Equifax is one of three major credit reporting bureaus in the United States, which aggregate the financial and personal information of consumers. Stacey Cowley & Tara Siegel Bernard, *As Equifax Amassed Ever More Data, Safety Was a Sales Pitch*, N.Y. TIMES (Sept. 23, 2017), https://nyti.ms/2yj1M4Y [https://perma.cc/A3XX-9S2N]. Equifax uses this information to create credit reports and profiles that are analyzed and sold to businesses—including banks, credit card companies, and employers—to determine individuals' financial risk. *Id.*

2. Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth & Ron Lieber, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sept. 7, 2017), https://nyti.ms/2xS95kJ [https://perma.cc/3BMP-N6GZ]. Since then, this number has been reestimated at approximately 145.5 million. Stacy Cowley, *2.5 Million More People Potentially Exposed in Equifax Breach*, N.Y. TIMES (Oct. 2, 2017), https://nyti.ms/2xPEFA2 [https://perma.cc/KGH4-N79A].

3. *U.S. and World Population Clock*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/ [https://perma.cc/8TUS-36SU]. If we assume that the breach primarily affected adults, this percentage would be higher because there are approximately 254 million people over the age of eighteen in the U.S. *See id.*

4. Tara Siegel Bernard & Stacy Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, N.Y. TIMES (Oct. 3, 2017), https://nyti.ms/2yFriRZ [https://perma.cc/9A78-LH8T].

5. *Id.*

6. *Id.*

7. Mike Isaac & Sheera Frenkel, *Facebook Security Breach Exposes Accounts of 50 Million Users*, N.Y. TIMES (Sept. 28, 2018), https://nyti.ms/2OmvHom [https://perma.cc/BH4E-3BCE];

cannot "opt-out" of the credit reporting industry and therefore have little control over their data.[8] Although there is already some industry regulation under the Fair Credit Reporting Act,[9] the Equifax breach prompted congressional leaders on both sides of the aisle to quickly express their support for stricter standards of privacy.[10] Despite the alarm raised by several high-profile breaches, consumers have become so accustomed to these incidents that a term has been coined to describe their prevalence and the resulting ennui: "data breach fatigue."[11]

Yet, there are myriad reasons to be wary of the growing frequency of data breaches. The Ponemon Institute, an independent research center that conducts yearly data breach analyses, estimated that there were, on average, 130 successful breaches *per company* in 2017.[12] This is a 27 percent increase from 2016, translating into an average cost of $11.7 million per organization for cybercrime attacks.[13] For consumers, this inevitably increases the possibility of identity theft and fraud if personal information is exposed in the breaches. According to one study, 16.7 million U.S. consumers fell prey to identity fraud in 2017, resulting in approximately $16.8 billion stolen.[14] Identity fraud schemes

---

Keith Collins, *Yahoo and Equifax Just Proved That You Can Never Trust the First Number Announced in a Data Breach*, QUARTZ (Oct. 23, 2017), https://qz.com/1093399/the-equifax-efx-and-yahoo-hacks-are-further-proof-that-you-should-never-trust-the-first-number-announced-in-a-data-breach/ [https://perma.cc/MRU9-BVW8].

8. Bernard & Cowley, *supra* note 4; *see also* Robert B. Avery et al., *An Overview of Consumer Data and Credit Reporting*, 89 FED. RES. BULL. 47, 48 (2003) (providing further insight on the credit reporting industry and consumer rights).

9. Fair Credit Reporting Act of 1970, Pub. L. No. 91–508, 84 Stat. 1128 (codified as amended at 15 U.S.C. §§ 1681–1681x (2012)).

10. AnnaMaria Andriotis, Michael Rapoport & Christina Rexrode, *Senators Rip Credit-Reporting Model in Wake of Equifax Breach*, WALL ST. J. (Oct. 4, 2017), https://www.wsj.com/articles/senators-rip-credit-reporting-model-in-wake-of-equifax-breach-1507136171 [https://perma.cc/X9H2-456R].

11. *See* Elise Hu, *I Feel Nothing: The Home Depot Hack and Data Breach Fatigue*, NPR (Sept. 8, 2014), http://www.npr.org/sections/alltechconsidered/2014/09/03/345539074/i-feel-nothing-the-home-depot-hack-and-data-breach-fatigue [https://perma.cc/745Q-CQYX] (discussing the disillusionment that consumers feel when retailers are hacked and credit card information is exposed).

12. PONEMON INST. & ACCENTURE, 2017 COST OF CYBER CRIME STUDY: INSIGHTS IN THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE 4 (2017), https://www.accenture.com/t20171006T095146Z__w__/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf [https://perma.cc/7E2N-MZUV].

13. *Id.* at 2.

14. *Facts + Statistics: Identity Theft and Cybercrime*, INS. INFO. INST. (2018), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime [https://perma.cc/26KB-5MQK]. These statistics are overall identity fraud figures and not solely based on identity

include employment fraud, tax fraud, credit card fraud, and creating new accounts.[15] For reference, when the state of Utah suffered a major data breach in 2012 that exposed 800,000 Utahans' personal information, an independent research agency estimated that more than 120,000 cases of fraud would result.[16] The agency projected the breach would cost each individual "more than $3,300 in losses, on average" with about "20 hours and $770 on lawyers and time lost from work to resolve the case."[17]

Former FBI Director Robert Mueller, speaking at a cyber security conference in 2012, presciently summarized the data breach landscape when he said, "there are only two types of companies: those that have been hacked and those that will be."[18] Assuming Mueller is correct and data breaches are inevitable, the question then becomes: What measures can be taken to minimize the risk of consumers' personal information being exposed by these attacks?

In the private sector, companies are responsible for safeguarding their customers' data and implementing adequate cybersecurity measures to prevent future attacks.[19] However, a study in the *Harvard Business Review* noted that "[d]irectors acknowledge cybersecurity as

---

fraud resulting from data breaches. *Id.* While some consider identity theft the unauthorized access to personal information and identity fraud the unauthorized *use* of that information for illicit gain, this Note will treat the two as interchangeable based on the Department of Justice's understanding of the terms. *See infra* note 56 and accompanying text.

15. *Id.* The Consumer Sentinel Network, which is maintained by the Federal Trade Commission and tracks consumer fraud and identity theft complaints, reported almost 2.7 million complaints in 2017. 2017 FED. TRADE COMM'N CONSUMER SENTINEL NETWORK DATA BOOK 3, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2017/consumer_sentinel_data_book_2017.pdf [https://perma.cc/6Y44-PNMQ]. The reports were divided between fraud (1.1 million), identity theft (371,000), and other (1.2 million). *Id.*

16. Ann Carrns, *The Cost to Consumers of a Data Breach*, N.Y. TIMES: BUCKS (Apr. 30, 2013), https://bucks.blogs.nytimes.com/2013/04/30/the-cost-to-consumers-of-a-data-breach/ [https://perma.cc/QV94-A4UM].

17. *Id.*

18. Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, Speech at the RSA Cyber Security Conference in San Francisco (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies [https://perma.cc/4ND8-2UZK].

19. *See, e.g.*, BANK OF AMERICA, *U.S. Consumer Privacy Notice* (Jan. 2018), https://www.bankofamerica.com/privacy/consumer-privacy-notice.go [https://perma.cc/L34U-KZHJ] ("To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."); *see also Enforcing Privacy Promises*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises [https://perma.cc/2C4F-7L4S] (listing recent FTC enforcement actions against companies for violating, among other things, privacy policies).

an urgent global issue, but are failing to make the connection between the pervasiveness of cyberthreats and their companies' vulnerabilities."[20] Most companies only discover deficiencies in their security systems following a data breach. Private parties then turn to litigation to bring claims for damages stemming from the breach and to demand better cybersecurity practices. For example, consumers may bring class action lawsuits or shareholders may bring securities fraud class actions and derivative suits.[21]

However, each of these litigation strategies face legal obstacles. Class action lawsuits are marred by standing problems due to a circuit split on the issue of what constitutes injury from a data breach.[22] When a company's stock price drops after a data breach, shareholders bringing securities fraud class actions have trouble demonstrating that they "relied to their detriment on a company's material misrepresentations" stemming from public statements and 10-K filings.[23] And derivative shareholder suits—targeting corporate boards and directors for allegedly breaching their fiduciary duties—are difficult to prove because of the high bar for successfully pleading demand futility and the power of the business judgment rule in Delaware courts.[24]

In the public sector, the regulatory framework for data breaches is comprised of a patchwork of rules and limited enforcement mechanisms. Hackers penetrate companies' computer systems to steal such precious data as financial information, trade secrets, or personally identifiable information ("PII"). In doing so, they violate numerous federal and state laws, like the Computer Fraud and Abuse Act.[25] In the medical field, the Health Insurance Portability and Accountability

20. J. Yo-Jud Cheng & Boris Groysberg, *Why Boards Aren't Dealing with Cyberthreats*, HARV. BUS. REV. (Feb. 22, 2017), https://hbr.org/2017/02/why-boards-arent-dealing-with-cyberthreats [https://perma.cc/96S4-R9M3].

21. *See* Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. B.J. 30, 30 (2016) (listing common types of cybersecurity breach litigation).

22. Megan Dowty, Note, *Life Is Short. Go to Court: Establishing Article III Standing in Data Breach Cases*, 90 S. CAL. L. REV. 683, 686 (2017).

23. Hooker & Pill, *supra* note 21, at 32.

24. For further discussion of shareholder derivative suits, see *infra* Part II.A.2.

25. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. 98–473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)). *See also* CHARLES DOYLE, CONG. RESEARCH SERV., 97-1025, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS 1 (2014).

Act of 1996[26] ("HIPAA") sets standards for storing medical information.[27] The Gramm-Leach-Bliley Act[28] ("GLBA") does the same for financial institutions using clients' nonpublic personal information.[29] Notably, there is no comprehensive national data security law. Instead, state attorneys general may charge companies for violating various state laws. All fifty states have data security laws, but most states only set standards for notifying consumers after data breaches.[30] Finally, the Federal Trade Commission ("FTC"), as the primary agency tasked with consumer protection, may bring enforcement actions against companies failing to safeguard consumer data.[31] While these actions may result in companies instituting new corporate governance practices or paying penalties, the FTC has remained conservative in its enforcement approach.[32]

Most of these remedies are retroactive. Though the fear of lawsuits may trigger some companies to institute cybersecurity reforms, drastic changes are needed to ensure that consumers' personal and financial information remains protected from increasing exposure. As companies continue to amass consumer information, and the effects of data breaches are magnified, this vulnerability has become a pressing public issue requiring immediate legislation.

This Note expands on the growing literature of proactive solutions in the wake of increasing data breaches, and argues that the current measures for dealing with data breaches are deeply inadequate. Instead of ex ante solutions, a forward-looking federal data security statute is imperative for protecting consumers' personal information. This statute should be modeled after laws such as HIPAA and GLBA, establish minimum cybersecurity standards, and detail best practices for companies that store consumer data. But this only addresses one

---

26. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

27. 42 U.S.C. § 1320d-6 .

28. Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

29. 15 U.S.C. §§ 6801–6809.

30. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Mar. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/KCD8-6K6Q].

31. *See* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2231 (2015) (discussing the developing regulatory role of the FTC).

32. *See id.* at 2235–36 ("Political considerations and the newness of privacy and data security issues may justifiably explain the FTC's modest approach.").

side of an admittedly complex issue—that of the companies who are already in possession of PII. A proactive solution also requires reconsidering how to minimize this growing problem by going to its source: the collection of PII in the first place. This Note will touch on two potential proactive solutions. One such solution is legislation regulating companies' collection and use of Social Security numbers ("SSNs"), which have arguably become the most valuable piece of PII. A second option is creating a decentralized, yet more secure system of identification—utilizing blockchain or a similar distributed ledger technology—to better protect consumers and provide them greater control over their data.[33]

Part I introduces the issues surrounding the exposure of personal data like Social Security numbers in data breaches. Part II expands on the current private and public regulatory framework in response to these breaches. These reactionary mechanisms have become ineffectual for instituting noticeable changes in this field. Finally, Part III argues that a federal data security statute is necessary and provides a better solution than the current patchwork of state laws. It also engages with two options for mitigating companies' reliance on Social Security numbers as personal identifiers.

I. DATA BREACHES AND THE VALUE OF PERSONAL INFORMATION

As the number of successful data breaches continues to rise, the risk to consumers' personal and financial information increases. Data breaches occur when "an individual name plus a Social Security number, driver's license number, medical record or financial record (credit/debit cards included) is potentially put at risk because of exposure" through either electronic or paper means.[34] According to the Identity Theft Resource Center, 9,395 data breaches were documented in the U.S. between January 1, 2005 and September 30, 2018, which

33. This solution aligns with the ongoing academic conversation about cyber privacy and how companies store and protect data. *See, e.g.*, Julia N. Mehlman, *If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information: A Look at the Data-Collection Industry and a Proposal for Recognizing the Value of Consumer Information*, 81 BROOK. L. REV. 329, 329 (2015) (examining the lack of regulation surrounding the data-collection industry and data brokers in general); Theodore Rostow, *What Happens When an Acquaintance Buys Your Data?: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. REG. 667, 691 (2017) (discussing the ability of individuals to buy consumer information and the resulting privacy harms).

34. *Data Breaches*, IDENTITY THEFT RESOURCE CTR., http://www.idtheftcenter.org/Data-Breaches/data-breaches [https://perma.cc/M6AG-RXBQ].

resulted in the exposure of more than one billion records.[35] These breaches are not confined to specific industries, but include attacks on banks, retailers, entertainment companies, healthcare providers, and even the federal government.[36]

There is no escaping the reality that personal data is the "new oil"—a valuable resource that has developed into a uniquely coveted asset.[37] Modern companies control troves of data containing consumers' PII. The literature on data brokers—companies that maintain personal data to analyze, package, and sell to marketers and other companies for targeting existing and potential customers—is extensive and growing in academia and through governmental inquiry.[38] Consumers can benefit from the increased accumulation of data by receiving personalized marketing experiences and innovative product offerings.[39] However, the same consumers have little control over how this information is utilized because most data brokers are not consumer-facing and their control over this data may diminish consumers' ability to seek insights into how their data is being used,

35. Records may include SSNs, credit/debit card numbers, protected health information, etc. *Id.* These data breach figures are based on the Identity Theft Resource Center's analysis of breaches "confirmed by various media sources and/or lists from state government agencies." *Id.* Of course, it remains a challenge to correctly assess the exact number of yearly data breaches. This information may not be regularly released and some companies may only publicly disclose a breach months after the incident.

36. Leslie R. Caldwell, Assistant Attorney Gen., Remarks at Roger Williams University School of Law Symposium: "Cybersecurity + Law Enforcement: The Cutting Edge" (Oct. 16, 2015), http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-cybersecurity-law [https://perma.cc/XP4L-RAVD].

37. *Personal Data: The Emergence of a New Asset Class*, WORLD ECONOMIC FORUM (Jan. 2011), http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf [https://perma.cc/A67V-ESRX] (quoting Meglena Kuneva, European Consumer Commissioner (Mar. 2009)).

38. *See, e.g.*, FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i (2014), http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/5MXD-SHF7] (reporting on the data collection practices of nine data brokers to shed light on the industry); MAJORITY STAFF OF S. COMM. ON COMMERCE, SCI., AND TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKERS INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES i (2013), http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577l [https://perma.cc/AF4M-FURJ] (focusing on the collection and sale of data for marketing purposes); Mehlman, *supra* note 33, at 331–32 (defining data brokers and their ability to easily collect and sell personal information).

39. FED. TRADE COMM'N, *supra* note 38, at v.

and to modify that usage.[40] Companies have few incentives to change these practices because, in the aggregate, this information is worth billions; JPMorgan Chase estimated that a "unique user was worth $4 to Facebook and $24 to Google."[41] And SEC filings put Facebook's figure closer to $120 per user.[42] In short, personal information has become big business.

As the accumulation and commercialization of arguably innocuous personal information, such as our spending patterns or "Likes" on Facebook, becomes controversial,[43] it follows that the mass collection of SSNs is even more problematic. SSNs are nearly-universal identifiers used by government agencies and businesses alike for record-keeping and financial monitoring.[44] In 1935, the Social Security Act was passed to establish a national system of old-age benefits.[45] The SSN was created to "uniquely identify U.S. workers, enabling employers to submit accurate reports of covered earnings for use in administering benefits under the new Social Security program."[46] Thirty-five million Americans received SSNs as a result of the original push by the Social Security Administration.[47]

However, the role of SSNs has expanded far beyond its original singularly intended use.[48] SSNs have become "skeleton keys," swiftly opening the door to identity theft following data breaches, which may

40. *Id.* at vi (commenting on data brokers' lack of transparency and noting that "even those consumers who know who the data brokers are, find their websites, and take the time to find the opt out and use it may still not know its limitations").

41. Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. TIMES (Feb. 12, 2012), https://nyti.ms/2vjGnK1 [https://perma.cc/4FUH-JUZA].

42. *Id.*

43. *See, e.g.*, Andrew Prokop, *Cambridge Analytica Shutting Down: The Firm's Many Scandals, Explained*, VOX (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/21/17141428/ cambridge-analyticar-trump-russia-mueller [https://perma.cc/9FAJ-QZGC] (detailing the Cambridge Analytica incident in which the British firm collected Facebook users' personal information for politically-motivated reasons).

44. Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SECURITY BULL., no. 2, 2009, at 1, 55.

45. *Id.*

46. *Id.* at 57.

47. *Id.* at 59. This included the distribution of Social Security cards. *Id.* at 57. The first three digits of the SSN represented the area number (assigned by geographical region), the next two were the group number (related to the order assigned in each area), and the last four were the serial number (numerical series from 0001-9999). *Id.* On June 25, 2011, the Social Security Administration changed this assignment procedure to a randomized system. *Social Security Number Randomization*, SOC. SECURITY. ADMIN., https://www.ssa.gov/employer/randomization.html [https://perma.cc/3DBE-7T9Q].

48. Puckett, *supra* note 44, at 69.

result in financial losses, detrimental impacts to credit scores, or even health insurance repercussions from fraudulently procured medical treatments.[49] Since there are no broad restrictions in federal law limiting the use of SSNs by the private sector, businesses regularly use the number as a form of personal identification.[50] While Social Security cards themselves have become resistant to counterfeiting, the number remains a "convenient means of identifying people in large systems of records."[51] Banks, credit card companies, employers, insurance agencies, schools, and even the local gym are just a few of the potential companies that may have a person's SSN on file.[52] Since data brokers buy and sell consumers' information, there are likely countless other businesses that have access to consumers' SSNs. To the surprise of many, these transactions may occur even if the consumer never authorized its disclosure to the selling party.[53] There are even striking instances in which data brokers sold this information to scammers directly.[54]

The ubiquity of the SSN as an identifier makes it a primary target for both hackers and identity thieves.[55] Identity theft and fraud occur when someone wrongfully obtains and uses another person's personal data, like a SSN, through fraud or deception for personal gain.[56] When data breaches expose SSNs, thieves can use these numbers—usually combined with other pieces of data—to impersonate individuals and

49. Adam Levin, *It's 10 p.m. Do You Know Where Your Social Security Number Is?*, HUFFINGTON POST (Jan. 7, 2015), https://www.huffingtonpost.com/adam-levin/its-10-pm-do-you-know-whe_b_6118342.html [https://perma.cc/Q8TE-3NWR].

50. Puckett, *supra* note 44, at 67.

51. *Id.*

52. Levin, *supra* note 49.

53. *See* Alex Schneider, *How Could They Know That? Behind the Data That Facilitates Scams Against Vulnerable Americans*, 19 VA. J.L. & TECH. 716, 717 (2015) (highlighting the dearth of regulation that allows data brokers to sell information without consumers' knowledge or consent).

54. *See, e.g.*, *Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers*, FED. TRADE COMM'N (Feb. 18, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive [https://perma.cc/XY23-QN5P] (describing a settlement against data brokers for knowingly selling the personal information of hundreds of thousands of consumers).

55. *See* Jonathan J. Darrow & Stephen D. Lichtenstein, *"Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J.L. & TECH. 1, 9 (2008) ("There is no doubt that the social security number is central to the commission of the crime of identity theft.").

56. *What Are Identity Theft and Identity Fraud?*, U.S. DEP'T. JUSTICE (Feb. 7, 2017), https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud [https://perma.cc/7WP9-Z3FN].

apply for loans, housing, utilities, or government benefits.[57] Additionally, this information may be sold on the black market to other hackers.[58] To compound things further, the average cost for each lost or stolen record containing sensitive and confidential information is approximately $148 per company, because of costs ranging from hiring forensic experts and in-house investigation teams to providing free credit monitoring services for affected customers.[59] While identity theft is illegal,[60] it has become increasingly difficult to catch these thieves and subsequently prosecute them due to jurisdictional challenges and attribution issues when pursuing foreign hackers.[61]

The high value placed on collecting personal information and its ubiquity in society amplify the potential harm caused by data breaches and identity theft. Until the collection, storage, and use of SSNs and other identifiers are controlled through regulation, personal information will likely continue to be unlawfully released.

II. THE CURRENT REGULATORY FRAMEWORK

The current legal and institutional framework for responding to and preventing data breaches is an expanding field. In the private sector, consumers and shareholders may file lawsuits against hacked companies to provoke changes in their data security systems and recover any damages from exposed personal information. However, these ex post responses invariably face procedural and substantive legal challenges. In the public sector, the federal options are only marginally better. There are existing mechanisms for holding companies accountable in specific fields, such as HIPAA and GLBA,

57. Craig Timberg, *How Equifax Hackers Might Use Your Social Security Number to Pretend They're You*, WASH. POST (Sept. 7, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/08/how-equifax-hackers-might-use-your-social-security-number-to-pretend-theyre-you/?utm_term=.c229b683d40f [https://perma.cc/D3CW-738H].

58. *Id.*; *see also* Keith Collins, *Here's What Your Stolen Identity Goes for on The Internet's Black Market*, QUARTZ (July 23, 2015), https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/ [https://perma.cc/98UD-FDNH] (analyzing the listings of personal information on a black-market website and concluding that the going rate for a stolen identity is about $20).

59. PONEMON INST. & IBM SEC., 2018 COST OF A DATA BREACH STUDY: GLOBAL OVERVIEW 8 (2018), https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf [https://perma.cc/LUL6-VU7F].

60. Identity Theft and Assumption Deterrence Act, 18 U.S.C. § 1028 (2012).

61. *See* Morgan Chalfant, *Feds Find Some Foreign Hackers Are Out of Reach*, HILL (Nov. 29, 2017), http://thehill.com/business-a-lobbying/362458-feds-find-some-foreign-hackers-are-out-of-reach [https://perma.cc/ZKK8-V9QU] (discussing the challenges of attributing these attacks to specific individuals and then extraditing them to the U.S. to face criminal charges).

and limited enforcement options through the FTC. Some states, such as California, Massachusetts, and New York, are at the forefront of proactive data security and breach legislation. Nevertheless, because no uniform system exists, most companies are free to set their own standards for using personal information and responding to these breaches.

A. Legal Hurdles of Private Litigation

After a data breach, two potential avenues for recovery are consumer lawsuits and shareholder lawsuits. However, the law with respect to these private litigation options is still developing and remains uncertain, leaving them as unsatisfactory solutions to a growing crisis.

1. *Consumer Lawsuits*. Consumers regularly file a variety of lawsuits in the wake of data breaches.[62] Class action lawsuits are the most publicized. However, issues persist because of the standing requirement under Article III of the U.S. Constitution.[63] For a successful data breach claim, a plaintiff must show: "(1) she suffered an 'injury in fact,' (2) her injuries were 'fairly traceable' to [the] defendant's actions, and (3) a favorable judgment will redress her injuries."[64] This "injury-in-fact" must be "concrete and particularized" and "actual or imminent."[65] Even if personal information is exposed, the actual injury may not have occurred yet.[66] To establish an injury, most courts have required allegations that the stolen data was used or

62. *See* Todd H. Greene, William A. Delgado & Nicole A. Diaz, *A Crash-Course in Data-Security Regulation and Litigation*, 33 ACC DOCKET 92, 97–98 (2015) (examining potential federal claims based on the Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse Act; state claims stemming from violations of state data privacy regulations and consumer protection statutes; and common law claims such as breach of contract, false advertising, and negligence).

63. U.S. CONST. art. III.

64. Eric S. Boos, Chandler Givens & Nick Larry, *Damages Theories in Data Breach Litigation*, 16 SEDONA CONF. J. 125, 127 (2015) (citing Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012)).

65. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

66. *See* Boos et al., *supra* note 64, at 127 (noting that "actual identity theft and a resulting loss of money or property" may be absent following a breach). Based on the recent Supreme Court case, *Clapper v. Amnesty International USA*, 568 U.S. 398, 398 (2016), proving future injury has become extraordinarily difficult. *See* Dowty, *supra* note 22, at 687–88 (discussing the high burden for standing imposed by *Clapper* and noting that "[c]ourts have since used *Clapper* to dismiss data breach actions for failing to show a recognizable injury").

its use was imminent.[67] Given the difficulty in tracking stolen data after a breach, this requirement is a stringent one for plaintiffs to satisfy.

In response, consumers have asserted alternative theories to prove injury. Some plaintiffs have successfully argued that data breaches caused injury through an increased risk of identity theft.[68] However, other plaintiffs have not fared as well because many courts have been reluctant to find the increased risk of future harm sufficient for standing without allegations that the plaintiffs suffered any actual harm.[69] For example, courts in the First and Third Circuits rejected this increased risk theory and have only recognized actual identity theft or fraud to confer standing.[70] Similarly, in the Fourth Circuit a panel recently found that the plaintiffs' allegations of harm from the increased risk of future identity theft "failed to establish a non-speculative, imminent injury-in-fact for purposes of Article III standing."[71] The U.S. District Court for the District of Columbia dismissed a significant case regarding the U.S. Office of Personnel Management breach based on similar reasoning.[72] Thus, until the Supreme Court weighs in, plaintiffs in many circuits will face almost

67. *In re* Zappos.com, Inc., 108 F. Supp. 3d 949, 955 (D. Nev. 2015), *rev'd*, 888 F.3d 1020 (9th Cir. 2018) (collecting data breach cases post-*Clapper* and noting that most courts have held that "absent allegations of actual identity theft or other fraud, the increased risk of such harm alone is insufficient to satisfy Article III standing"); Dowty, *supra* note 22, at 688.

68. *See, e.g.*, *In re* Zappos.com, Inc., 888 F.3d 1020, 1023 (9th Cir. 2018) (reversing the district court's dismissal because the plaintiffs sufficiently alleged Article III standing based on the risk of identity theft); *see also* Galaria v. Nationwide Mut. Ins. Co., 663 Fed. App'x 384, 389 (6th Cir. 2016) (holding that data breach victims satisfied the injury-in-fact requirement); Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (holding that data breach victims satisfied the injury-in-fact requirement because they faced a "credible threat of real and immediate harm").

69. Dowty, *supra* note 22, at 689; *see also* Reilly v. Ceridian Corp., 664 F.3d 38, 43 (3d Cir. 2011) ("Appellants in this case have yet to suffer any harm, and their alleged increased risk of future injury is nothing more than speculation.").

70. Dowty, *supra* note 22, at 689–90; *see also* Katz v. Pershing, LLC, 672 F.3d 64, 80 (1st Cir. 2012) (finding that, because the plaintiff did "not identify any incident in which her data has ever been accessed by an unauthorized person," her omission was "fatal" for satisfying Article III standing).

71. Beck v. McDonald, 848 F.3d 262, 267, 272–75 (4th Cir. 2017) (finding that the plaintiffs failed to show that the risks were substantial and the identity theft was not "certainly impending").

72. *See In re* U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 266 F. Supp. 3d 1, 9 (D.D.C. 2017) ("Neither the Supreme Court nor the U.S. Court of Appeals for the D.C. Circuit has held that the fact that a person's data was taken is enough by itself to create standing to sue . . . ."). *But see* Attias v. Carefirst, Inc., 865 F.3d 620, 629–30 (D.C. Cir. 2017) (finding that the plaintiffs' allegation of the threat of harm from a data breach was enough to satisfy the "injury in fact" standing requirement).

certain dismissal of their claims and find themselves unable to seek a legal remedy.

Another unsuccessful approach has been for plaintiffs to argue that a breach devalues their personal information.[73] The core of this "reduced value" theory is that personal information is inherently valuable and a breach "deprives the plaintiff[s] of that value."[74] While this theory has been accepted by some courts, especially in the Ninth Circuit,[75] many other courts have rejected this theory.[76] For example, plaintiff-customers brought a class action against Barnes & Noble after a security breach in which "skimmers" stole customer credit card and debit information.[77] They claimed, among other things, that this breach resulted in a deprivation of the value of their PII.[78] The court rejected this theory as insufficient to establish standing, instead finding that "[a]ctual injury of this sort is not established unless a plaintiff has the ability to sell his own information and a defendant sold the information."[79] Other courts have reached similar conclusions.[80]

Plaintiffs have tried to pursue a third theory of standing: arguing that a portion of their payment to access a service was necessarily earmarked for data security through a contract, and because defendant's data security was negligent, the plaintiffs were defrauded of that money.[81] So, plaintiffs have alleged an "overpayment" equal to

---

73. *See* Boos et al., *supra* note 64, at 135–36 (observing the limited success of this approach in data breach cases).

74. *Id.* at 135.

75. *See, e.g.*, *In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, at *13–14 (N.D. Cal. Aug. 30, 2017) (noting that "the Data Breaches caused all Plaintiffs to suffer a loss of value of their PII as a result of the Data Breaches"); *In re* Anthem, Inc. Data Breach Litig. ("Anthem II"), No. 15-MD-02617-LHK, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (finding that the plaintiffs sufficiently pleaded damages); Claridge v. RockYou, Inc., 785 F. Supp. 2d 855, 861 (N.D. Cal. 2011) (holding that the defendant's control over the plaintiff's PII was valuable property and therefore, the plaintiff should be responsible for the potential loss in value).

76. *See* Boos et al., *supra* note 64, at 136 n.38 (collecting cases dismissing the reduced value theory).

77. *In re* Barnes & Noble Pin Pad Litig., No. 12-CV-8617, 2013 WL 4759588, at *1 (N.D. Ill. Sept. 3, 2013).

78. *Id.* at *5.

79. *Id.*

80. Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 875 (N.D. Ill. 2014); Yunker v. Pandora Media, Inc., 11–CV–03113 JSW, 2013 WL 1282980, at *4 (N.D. Cal. Mar. 26, 2013); Low v. LinkedIn Corp., No. 11-CV-01468-LHK, 2011 WL 5509848, at *4 (N.D. Cal. Nov. 11, 2011).

81. *See* Boos et al., *supra* note 64, at 141–42 (detailing the novelty and contours of the "overpayment" theory).

the premium paid to defendants for their alleged data security.[82] However, this "overpayment" theory has generally been rejected too.[83]

Even if the plaintiffs overcome the standing hurdle, complications abound.[84] For example, in *In re iPhone Application Litigation*,[85] the Northern District of California found that mobile device manufacturers' alleged violations of the Stored Communications Act and Apple's further violations of the Wiretap Act—both based on unauthorized personal data collection and tracking—were sufficient to confer standing under the respective statutes.[86] Nonetheless, the allegations were ultimately dismissed for failure to state a claim under the statutes.[87] Cases like *In re Hulu Privacy Litigation*[88] also highlight potential class certification problems. Hulu customers claimed that their personal information was wrongly disclosed to third parties and successfully demonstrated this injury based on the Video Privacy Protection Act.[89] Yet, the court denied class certification because the plaintiffs could not overcome the threshold issue of establishing and ascertaining a definable class.[90]

So, federal courts have become a de facto roadblock for many litigants bringing data breach claims. The few success stories are overshadowed by the litany of courts unwilling to expand the reach of

82. *Id.* at 142.

83. *See, e.g.*, *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 643 (3d Cir. 2017) (Shwartz, J., concurring) (noting that the overpayment theory is "not sufficient to provide standing in the context of data thefts" and collecting cases where "courts have rejected" the theory); Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963, 968 (7th Cir. 2016) (finding standing on other grounds, but declining "to push [overpayment] theory beyond its current scope"). *But see* Svenson v. Google Inc., No. 13-CV-04080-BLF, 2015 WL 1503429, at *4 (N.D. Cal. Apr. 1, 2015) (finding that the plaintiff had "alleged facts sufficient to show contract damages under a benefit of the bargain theory").

84. For a brief overview of data breach litigation trends in 2017, see Client Release, Gibson, Dunn & Crutcher LLP, U.S. Cybersecurity and Data Privacy Outlook and Review – 2018, at 25–34 (Jan. 25, 2018), https://www.gibsondunn.com/wp-content/uploads/2018/01/us-cybersecurity-and-data-privacy-outlook-and-review-2018.pdf [https://perma.cc/64GT-5CNL].

85. *In re* iPhone Application Litig., 844 F. Supp. 2d 1040 (N.D. Cal. 2012).

86. *Id.* at 1054–55.

87. *Id.* at 1056–62 (dismissing the Stored Communications Act and Wiretap Act arguments after the court narrowly interpreted the respective statutes to exclude the defendants and their electronic activities).

88. *In re* Hulu Privacy Litig., No. C 11-03764 LB, 2012 WL 2119193 (N.D. Cal. June 11, 2012).

89. *Id.* at *5, *8.

90. FED. R. CIV. P. Rule 23(c)(1)(B) ("An order that certifies a class action must define the class and the class claims, issues, or defenses."); *In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 WL 2758598, at *15 (N.D. Cal. June 17, 2014) ("Plaintiffs have offered no way to identify individual class members other than broad notice and a self-reporting affidavit.").

consumers' legal theories, thus preventing monetary recovery and hindering substantive changes in cybersecurity practices.

2. *Shareholder Lawsuits*. After a data breach, shareholders may file actions against companies for losses sustained post-breach through two methods: securities fraud class actions and derivative shareholder suits.[91] However, recent developments in Delaware corporate law have created high barriers to prove these claims. Additionally, since many of these lawsuits are drawn-out endeavors driven primarily by plaintiffs' counsel, any potential recovery is minimized.

First, potential plaintiffs bring securities fraud class actions when disclosures of data breaches are followed by a noticeable drop in a company's share price.[92] These claims typically arise from Sections 10(b) of the Securities Exchange Act of 1934 and SEC Rule 10b-5,[93] and require plaintiffs to prove that the defendants "(1) made misstatements or omissions of material fact; (2) with scienter; (3) in connection with the purchase or sale of securities; (4) upon which plaintiffs relied; and (5) that plaintiffs' reliance was the proximate cause of their injury."[94]

In data breach cases, shareholders typically allege that they relied on either a company's pre-breach public disclosures, which understated data security risks or overstated cybersecurity protections, or the company withheld or was too slow in revealing the breach.[95] These fraud theories cover buyers who bought shares prior to a breach and those who sold in the period between the date of the breach and its disclosure.[96] Since these disclosures typically decrease the share price, a shareholder's potential recovery becomes the difference between the price paid by the buyer (or sold by the seller) and the market price after corrective disclosure.[97]

---

91. Kimberly R. Hillman & Collin J. Hite, *Has the Fortress Been Hacked by Consumers? Cyber Class Actions Are Gaining Steam*, ACC DOCKET, May 2016, at 62, 66.

92. *Id.*

93. 15 U.S.C. § 78j(b) (2012); 17 C.F.R. § 240.10b-5 (2016).

94. Weiner v. Quaker Oats Co., 129 F.3d 310, 315 (3d Cir. 1997) (internal quotation marks omitted).

95. Derek Borchardt & Craig A. Newman, *The Next Big Thing: Data Breach Securities Class Action Litigation*, PATTERSON BELKNAP: DATA SECURITY LAW BLOG (Feb. 20, 2018), https://www.pbwt.com/data-security-law-blog/the-next-big-thing-data-breach-securities-class-action-litigation [https://perma.cc/GF3D-A8WJ].

96. *Id.*

97. RICHARD A. BOOTH, FINANCING THE CORPORATION § 9:32 (2017).

This litigation strategy has seen mixed results. For example, in 2009, shareholders brought a securities fraud class action against Heartland Payment Systems after the company's stock dropped by 80 percent following the revelation of a data breach two years earlier in 2007.[98] The shareholders claimed that Heartland's management made materially fraudulent statements by continuing to assert the adequacy of its data security on investor calls and through its 10-K filings after the earlier breach.[99] The district court ultimately dismissed the complaint because Heartland emphasized a high level of security and promptly announced the breach to shareholders when it discovered its full impact.[100] Similarly, when Yahoo's stock price dropped in 2016 after the company publicly disclosed massive data breaches from 2013 and 2014, shareholders brought securities fraud lawsuits.[101] While these claims were convincing enough to encourage Yahoo to settle for $80 million,[102] this disposition isn't representative of a changing tide.[103] As *Heartland* indicates, litigants bringing these securities fraud claims will continue facing the high burden of proving actual material misrepresentations or omissions related to companies' security systems, and cannot rely on allegations of mere security inadequacies following a breach.[104]

Second, shareholders may bring derivative actions for breach of fiduciary duties. As a basic principle, boards of directors and officers owe fiduciary duties to their corporations and stockholders.[105] When making decisions, directors and officers are bound by the duties of care

98. *In re* Heartland Payment Sys., Inc. Sec. Litig., CIV. No. 09-1043, 2009 WL 4798148, at *1 (D.N.J. Dec. 7, 2009).

99. Hillman & Hite, *supra* note 91, at 66.

100. *Id.* (finding that the "mere fact of the security breach did not demonstrate that the company had failed to place appropriate emphasis on maintaining a high level of security").

101. Kevin LaCroix, *Yahoo Settles Data Breach-Related Securities Suit for $80 million*, D&O DIARY (Mar. 5, 2018), https://www.dandodiary.com/2018/03/articles/securities-litigation/yahoo-settles-data-breach-related-securities-suit-80-million/ [https://perma.cc/3PLX-J8H6].

102. *Id.*

103. *Id.* (arguing that "merely because the Yahoo case, with all of these distinctive features, resulted in a significant settlement does not necessarily mean that many other companies will be sued or that the plaintiffs' lawyers are going to be able to secure significant recoveries in a lot of other cases").

104. *In re* Heartland Payment Sys., Inc. Sec. Litig., CIV. No. 09-1043, 2009 WL 4798148, at *7 (D.N.J. Dec. 7, 2009).

105. *See* Guth v. Loft, Inc., 5 A.2d 503, 510 (Del. 1939) ("While technically not trustees, [corporate officers and directors] stand in a fiduciary relation to the corporation and its stockholders.").

and loyalty.[106] A corporate shareholder may bring a suit on behalf of the corporation to prove that the directors and officers breached a duty.[107] However, before this action, the shareholders must make a demand on the board of directors to bring the suit on the corporation's behalf, unless the shareholder can show such a demand would be "futile."[108] Courts take various approaches in evaluating demand futility,[109] but generally allow suits to proceed if the shareholder can show that the directors were either "too self-interested or too controlled by the alleged wrongdoers to make a valid business decision" regarding whether to proceed with the suit.[110]

In the context of data breaches, derivative claims are generally based on the "board's failure to maintain adequate security to prevent the breach, failure to take adequate measures to respond and report the breach, or both."[111] However, claims that the board breached its fiduciary duty of care based on cybersecurity practices have generally been denied in the pleading stage because of the business judgment rule, which offers directors a presumption that they have upheld their

106. Lucie F. Huger & Danielle Durousseau, *Director and Officer Liability for Data Breaches*, 30 WESTLAW J. CORP. OFFICERS & DIRECTORS LIABILITY, no. 24, 2016, at 1; *see also* William M. Lafferty, Lisa A. Schmidt & Donald J. Wolfe, Jr., *A Brief Introduction to the Fiduciary Duties of Directors Under Delaware Law*, 116 PENN ST. L. REV. 837, 842–49 (2012) (explaining each of these duties and their origins in depth). The duty of care "requires that directors inform themselves 'prior to making a business decision, of all material information reasonably available to them.'" *Id.* at 842 (citing Smith v. Van Gorkom, 488 A.2d 858, 872 (Del. 1985)). The duty of loyalty "requires a director to put the interests of the corporation and its stockholders ahead of the director's own personal interests which are not shared by the stockholders generally." *Id.* at 845 (citing Cede & Co. v. Technicolor, Inc., 634 A.2d 345, 361 (Del. 1993)). Related duties include good faith, confidentiality, and disclosure. *Id.* at 847–49.

107. FED. R. CIV. P. 23.1; Carole F. Wilder, *The Demand Requirement and the Business Judgment Rule: Synergistic Procedural Obstacles to Shareholder Derivative Suits*, 5 PACE L. REV. 633, 633 (1985).

108. *Wilder*, *supra* note 107, at 635. Courts have created a futility exception to the demand requirement, which allows plaintiff's demand requirement to be excused when it would have been "futile," "useless," or "unavailing." *Id.* at 636 (quoting Cathedral Estates v. Taft Realty Corp., 228 F.2d 85, 88 (2d Cir. 1955)).

109. *See generally* Jay M. Zitter, *Circumstances Excusing Demand Upon Board of Directors that is Otherwise Prerequisite to Bringing of Stockholder's Derivative Suit on Behalf of Corporation*, 43 A.L.R.6th 1 (Originally published in 2009) (compiling federal and state court shareholder derivative suits and evaluating courts' responses to whether shareholders' demands were excused as futile).

110. *Id.*

111. Daniel S. Strick et al., *Recent Developments Affecting Professionals', Directors', and Officers' Liability*, 51 TORT TRIAL & INS. PRAC. L.J. 635, 648 (2016).

fiduciary duties.[112] For example, courts have generally supported corporate boards that refuse to indulge shareholders' post-data breach derivative suits, so long as the board conferred with outside counsel and took steps to improve security after the breach.[113]

Litigants who bring suits against boards for breach of loyalty claims, such as failing to institute internal controls to prevent data breaches, have faced similar challenges because of the legal distinction between poor business judgment and bad faith in Delaware law. In a recent breach of loyalty suit against Home Depot following a data breach,[114] the plaintiffs failed to make a demand to the board, believing it to be futile.[115] In response, the Northern District of Georgia, applying Delaware law, noted that the plaintiffs were required to show "director conduct that [was] 'so egregious on its face that board approval [could not] meet the test of business judgment, and a *substantial likelihood* of director liability therefore exist[ed].'"[116] Combining the demand futility standard and the breach of loyalty claim meant the plaintiffs had to overcome a heavy burden and plead with particularized facts "that a majority of the [Home Depot] Board faced substantial liability," and therefore was not disinterested in the corporation's potential suit against the board "because it consciously failed to act in the face of a known duty to act."[117] Unsurprisingly, the plaintiffs failed to do so. Because the directors were only required to take "*any* course of action that was reasonable," the plaintiffs could not make a claim that the directors breached the duty of loyalty.[118] Here, that action was the

112. *See id.* at 644–45 ("The business judgment rule is a common law doctrine protecting directors and officers from liability when they make good faith business decisions in an informed and deliberate manner.").

113. *See, e.g.*, Palkon v. Holmes, No. 2:14-CV-01234 SRC, 2014 WL 5341880, at *1, *6 (D.N.J. Oct. 20, 2014) (finding that the board's refusal of the shareholder's demand was not based on bad faith or an unreasonable investigation and dismissing the case because of the business judgment rule's "strong presumption" in favor of not questioning the business decisions of boards); *see also* Brian J. Perreault, *Shareholder Derivative Lawsuits Spawning from Cyber Attacks*, 1 DATA SEC. & PRIVACY L. § 8:55 (2018) (discussing a derivative action against the retailer Target and eventual dismissal of the lawsuit because Target's outside Special Litigation Committee—which the court determined was disinterested and demonstrated good faith in its investigation—recommended not pursuing the derivative claim).

114. *In re* The Home Depot, Inc. S'holder Derivative Litig., 223 F. Supp. 3d 1317, 1320–21 (N.D. Ga. 2016).

115. *Id.* at 1324.

116. *Id.* at 1325 (quoting Aronson v. Lewis, 473 A.2d 805, 815 (Del. 1984)).

117. *Id.*

118. *Id.* at 1326.

Board's pre-breach plan to fix Home Depot's security weaknesses.[119] The court concluded that while the Board's implementation of this plan may have been slow and imperfect, unwise business judgments are not enough to plead bad faith, and thus the demand was not excused as to the breach of loyalty claims.[120] While an appeal was filed, the parties ultimately settled on April 28, 2017.[121]

Consequently, if directors and officers maintain *some* cybersecurity mechanisms, the company will likely be shielded from any liability. Unless there is a push for an increased cybersecurity fiduciary duty, Delaware law will remain a dead-letter for motivating companies to alter their cybersecurity practices. Additionally, shareholder derivative suits and securities fraud class actions appear driven by plaintiffs' counsel and their own profit motivations,[122] increasing the likelihood of settlement. Although some settlements may result in corporate governance reforms,[123] parties do not prioritize the protection of consumers' personal information. Therefore, they are unlikely to encourage significant changes in this field.

---

119. *Id.* at 1327.

120. *Id.*

121. Kevin LaCroix, *Home Depot Settles Data Breach-Related Derivative Lawsuit*, D&O DIARY (May 1, 2017), https://www.dandodiary.com/2017/05/articles/cyber-liability/home-depot-settles-data-breach-related-derivative-lawsuit/ [https://perma.cc/REM7-TMZP]. In a sign of the continued usage of these actions, shareholders of the Wendy's fast food restaurant recently filed their own derivative lawsuit with the intention of using the previous cases as a template to overcome the high hurdles they face in the demand stage. *See* Joseph B. Crace, Jr. & Virginia M. Yetter, *When Does Data Breach Liability Extend to the Boardroom?*, LAW360 (Apr. 3, 2017, 12:43 PM), https://www.law360.com/articles/907786 [https://perma.cc/RMB9-YCBT] (observing that the substantive allegations in the Wendy's suit are nearly identical to those in previous suits, but that the plaintiffs have provided more detailed allegations regarding demand futility).

122. *See* Jill E. Fisch, *Teaching Corporate Governance Through Shareholder Litigation*, 34 GA. L. REV. 745, 750 (2000) (finding that because plaintiffs' recovery is limited to damages, representative litigation does not create a substantial incentive for plaintiffs to litigate, but does incentivize the plaintiff's bar); *see also* LaCroix, *supra* note 121 (arguing that the plaintiff's bar is "very entrepreneurial" and is continuously testing the legal waters of these data breach cases).

123. Home Depot agreed to adopt cybersecurity corporate governance reforms and to pay up to $1.125 million in plaintiffs' attorneys' fees. LaCroix, *supra* note 121. It also agreed to document the duties and responsibilities of the Chief Information Security Officer and maintain an executive-level committee focused on data security. Plaintiffs' Unopposed Motion for Preliminary Approval of Shareholder Derivative Settlement and Memorandum of Law in Support at 2, *In re* The Home Depot, Inc. S'holder Derivative Litig., No. 1:15-CV-2999 TWT, 2017 WL 1830045, at *2 (N.D. Ga. Apr. 28, 2017).

B. Limited Public Laws and Enforcement Mechanisms

The current public regulatory framework is a patchwork of federal and state laws. As a national security issue, the U.S. government is working to prevent large-scale data breaches. This has become a coordinated effort between multiple agencies, such as the Department of Homeland Security,[124] the Department of Justice,[125] and the Securities and Exchange Commission.[126] However, there is no comprehensive federal data security legislation.[127] Instead, a series of overlapping state laws exist that regulate similar conduct (such as notification requirements for data breaches), but with state-specific variations (such as the timing or method of notice).[128] Additionally, the FTC seeks to protect consumers' information in the private sector through civil enforcement actions and policy initiatives.[129]

While many of these efforts are steps in the right direction for setting minimum cybersecurity standards, most remain reactive measures. First, two of the most robust federal laws protecting consumers' information are confined to the financial and healthcare sectors.[130] In the financial sector, GLBA contains provisions for cybersecurity liability for banks, securities firms, insurance companies, and other tangential companies.[131] Under GLBA, government

124. *Combating Cyber Crime*, U.S. DEP'T HOMELAND SECURITY (May 31, 2018), https://www.dhs.gov/topic/combating-cyber-crime# [https://perma.cc/ND9J-B5ZF] ("The Department of Homeland Security . . . conduct[s] high-impact criminal investigations to disrupt and defeat cyber criminals, prioritize the recruitment and training of technical experts, develop standardized methods, and broadly share cyber response best practices and tools.").

125. *See* Caldwell, *supra* note 36 ("[I]t is no surprise that the Attorney General has made clear that fighting cybercrime is one of the highest priorities of the Department of Justice.").

126. *Cybersecurity, the SEC and You*, U.S. SEC. EXCHANGE COMM'N (Oct. 2, 2017), https://www.sec.gov/spotlight/cybersecurity [https://perma.cc/BRM6-GC9B] ("The SEC uses its civil law authority to bring cybersecurity-related enforcement actions that protect investors, hold bad actors accountable and deter future wrongdoing.").

127. Greene et al., *supra* note 62, at 94.

128. *See Security Breach Notification Laws*, *supra* note 30 (listing security breach notification laws for each state).

129. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, FED. TRADE COMM'N: BUS. BLOG (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc [https://perma.cc/6FJ4-8KWL] ("The FTC has undertaken substantial efforts for well over a decade to promote data security in the private sector through civil law enforcement, business outreach and consumer education, policy initiatives, and recommendations to Congress to enact legislation in this area.").

130. While there are similar personal information and consumer protection statutes, such as The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (2012), and the Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012), this Note will focus on GLBA and HIPAA.

131. Gramm–Leach–Bliley Act §§ 501–510, 15 U.S.C. §§ 6801–6809 (2012).

agencies and authorities must "establish appropriate standards" for financial institutions to safeguard customers' personal financial information in order to: (1) "[e]nsure the security and confidentiality of customer records and information," (2) "protect against any anticipated threats or hazards to the security or integrity of such records," and (3) "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[132] In the health care sphere, HIPAA protects consumers' private medical information[133] when it is used by health care providers, data processors, pharmacies, and other companies with the need to access to medical information.[134] Violations of these privacy provisions may result in either civil or criminal liability.[135] HIPAA also has specific provisions for breach notification that allow the U.S. Department of Health and Human Services to bring civil actions for violations.[136]

In recent years, legislators have proposed several national data security provisions with little success. Connecticut Senator Richard Blumenthal introduced one of the most consumer-friendly bills, the Personal Data Protection and Breach Accountability Act of 2014.[137] This bill set data security standards for businesses collecting and using sensitive PII.[138] It also proposed civil and criminal penalties for companies failing to protect this information and notify consumers in a timely manner following a breach.[139] Similarly, Vermont Senator Patrick Leahy has sought passage of the Personal Data Privacy and

132. Gramm–Leach–Bliley Act, 3B Fed. Proc. Forms § 8:394 (2018).

133. *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.) (establishing HIPAA regulations).

134. Ieuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. L. (July 1, 2016), http://us.practicallaw.com/6-502-0467.

135. EDWARD F. MALONE, JENNER & BLOCK, LLC, "WHO GOES TO JAIL?" A GUIDE FOR HIPAA PRIVACY OFFICERS 1 (2002), http://www.ehcca.com/presentations/HIPAA3/malone_1.pdf [https://perma.cc/HB39-EQ33].

136. HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400–414 (2016).

137. Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014).

138. *Id.* § 202 (requiring business entities to implement a comprehensive program that: "(1) ensure[s] the privacy, security, and confidentiality of sensitive personally identifiable information; (2) protect[s] against any anticipated vulnerabilities to the privacy, security, or integrity of [such information]; and (3) protect[s] against unauthorized access to or use of [such information] that could create a significant risk of harm to any individual").

139. Brett V. Newman, *Hacking the Current System: Congress' Attempt To Pass Data Security and Breach Notification Legislation*, 2015 U. ILL. J.L. TECH. & POL'Y 437, 452 (2015).

Security Act[140] since 2005.[141] This bill would enact a federal security breach notification law and set standards for data and security programs.[142] However, these bills, and other similar pieces of legislation, have been met by continued resistance within Congress because of the divergent interests of businesses, state legislatures, and consumer advocacy groups.[143]

Second, the state-level laws on data security and breach notification that have been enacted and enforced by state attorneys general vary in substance and scope. Breach notification laws have been passed in fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.[144] Each state retains differences in these provisions, such as which companies must comply, definitions of "personal information," what constitutes a breach, and the requirements for notifying those affected by the breach.[145]

Currently, California has some of the most robust data security laws in the country. California's present privacy law applies to all persons, businesses, and state agencies in California that own or license personal information.[146] This is a broader definition than some states' laws that cover or exempt only certain types of companies.[147] In California, companies are required to publicize any breach of their security systems to all residents whose unencrypted personal

140. Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014).

141. Newman, *supra* note 139, at 449 (citing Eric Chabrow, *Why U.S. Breach Notice Bill Won't Pass*, BANK INFO. SEC. (Jan. 14, 2014), http://www.bankinfosecurity.com/blogs/us-breach-notice-bill-wont-pass-p-1602/op-1 [https://perma.cc/GSA7-5V2K]).

142. *See* Personal Data Privacy and Security Act of 2014, S. 1897, 113th Cong. (2014) (stating that the bill's purpose is "[t]o prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information").

143. *See* Joshua R. Eckert, *Passing Federal Security Breach Legislation: A "How-to Guide,"* 10 OHIO ST. BUS. L.J. 27, 47 (2015) (noting that businesses have rejected these laws for imposing burdens "above and beyond those that are implemented by most states," while state legislatures and consumer groups have been wary of federal legislation "that is not at least as protective of their citizens as their current state statutory scheme").

144. *See supra* note 30 and accompanying text.

145. *See supra* note 30 and accompanying text.

146. CAL. CIV. CODE § 1798.82 (2017).

147. *See, e.g.*, FLA. STAT. § 501.171 (2014) (covering commercial entities that maintain PII, but not individuals); GA. CODE ANN. § 10-1-912(a) (2010) (covering information brokers or data collectors that have personal information of individuals); ME. REV. STAT. ANN. tit. 10, § 1347(3) (2005) (covering information brokers that engage, "in whole or in part in the business of collecting . . . information concerning individuals for the *primary purpose* of furnishing personal information to nonaffiliated 3rd parties") (emphasis added).

information has been acquired by an unauthorized person.[148] Like many similar data laws, these only apply to California residents, and may not trigger any notification requirements for other similarly affected consumers.[149] However, in 2018 the California legislature passed the California Consumer Privacy Act (A.B. 375).[150] The new Act broadly defines personal information[151] and gives California consumers a multitude of privacy rights, including the right to know what personal information is being collected about them, the right to know whether that information is being sold or disclosed and to whom, and the right to opt out of the sale of that information.[152] Since the Act won't go into effect until January 2020, companies that collect personal information have time to analyze the law's implications and potentially propose limiting or clarifying amendments.[153]

Outside of California, most state laws remain reactionary because they have requirements for data breach notifications, but not regulations for information security protections.[154] While not as innovative as California, two states—Massachusetts and New York—are moving towards greater protection of personal information. Massachusetts' 2010 data security regulation applies to "[e]very person that owns or licenses personal information about a resident of the Commonwealth" and requires increased data security, such as instituting comprehensive information security programs, ensuring adequate security training for employees, and encrypting personal data.[155] While no private right of action exists for consumers, the Massachusetts state attorney general may bring claims against companies that violate this section.[156] In New York, the State

148. CAL. CIV. CODE § 1798.82.

149. *Id.* § 1798.82(a) ("A person or business that conducts business in California . . . shall disclose a breach of the security of the system . . . to a *resident of California* . . . ." (emphasis added)).

150. California Consumer Privacy Act of 2018, ch. 55, 2018 Cal. Stat. 91 (codified at CAL. CIV. CODE TIT. 1.81.5 (2018)) (effective Jan. 1, 2019).

151. CAL. CIV. CODE § 1798.140(o) (listing "personal information" as a consumer's personal identifiers, commercial information, biometric information, geolocation data, etc.).

152. *Id.* §§ 1798.100—120.

153. Dipayan Ghosh, *What You Need To Know About California's New Data Privacy Law*, HARV. BUS. REV. (July 11, 2018), https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law [https://perma.cc/L9VG-HP92].

154. *See* Jolly, *supra* note 134 (noting that early state breach notification laws tended to be "reactive" solutions).

155. 201 MASS. CODE REGS. § 17.03 (2009).

156. MASS. GEN. LAWS ch. 93H, § 6 (2018).

Department of Financial Services recently enacted the Cybersecurity Requirements for Financial Services Companies regulation for increased cybersecurity compliance in the financial sector.[157] Specifically, the regulation is "designed to promote the protection of customer information as well as the information technology systems of regulated entities."[158] The law requires covered entities to maintain a Chief Information Security Officer for overseeing and implementing cybersecurity programs.[159] It also requires the Board of Directors or a Senior Officer to sign off on these changes for compliance.[160] Notably, the New York regulation contains a private right of action, while the Massachusetts one does not. At bottom, both the New York and Massachusetts regulations are imperfect, but they nonetheless represent the progression toward stricter data security measures beyond California.

Third, while the FTC has become the de facto regulatory agency for cybersecurity enforcement, the agency has been relatively conservative in its approach.[161] This restraint may stem from the original uncertainty surrounding the FTC's power in the cybersecurity realm.[162] Recently, the FTC's ability to enforce cybersecurity claims was reaffirmed.[163] Section 5(a) of the FTC Act gives the FTC the ability to investigate "unfair or deceptive acts or practices."[164] For example, it is a "deceptive" practice if a company promises to securely maintain data and then experiences a breach resulting from inadequate standards.[165] An "unfair" practice would be if a company failed to adopt "industry-standard security measures."[166] This may include failures to maintain adequate log-in protocols, create data encryption procedures, or conduct cybersecurity training.[167]

---

157. N.Y. COMP. CODES R. & REGS. tit. 23, pt. 500 (2018).

158. *Id.* § 500.00.

159. *Id.* § 500.04.

160. *Id.* § 500 App'x A.

161. *See* Hartzog & Solove, *supra* note 31, at 2266 (arguing that the FTC has "developed its jurisprudence in a measured and modest way" and should strive for more proactive enforcement).

162. *Id.* at 2236–37.

163. *See id.* at 2240 (arguing that *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247–48 (3d Cir. 2015), upheld the FTC's power to regulate corporate cybersecurity through Section 5(a) of the FTC Act).

164. 15 U.S.C. § 45(a)(1) (2012).

165. Greene et al., *supra* note 62, at 94.

166. *Id.*

167. *Id.*

One notable victory for the FTC was against LifeLock, an identity theft protection agency, in 2015.[168] According to the FTC's filing, LifeLock violated a 2010 federal court order requiring the company to secure consumers' information and prohibiting deceptive advertising.[169] LifeLock failed to establish a comprehensive information security program and falsely advertised that it protected its consumers' personal information "with the same high-level safeguards used by financial institutions."[170] LifeLock was required to pay $100 million to consumers in settlement fees.[171] However, the FTC's reach has been limited to only the most egregious cases, such as LifeLock and the breach of the dating website Ashley Madison.[172] Some critics contend that the FTC is engaging in "a form of rulemaking . . . where it lacks meaningful rulemaking authority" by regulating cybersecurity practices.[173] But proponents of the FTC consider its de facto rulemaking an inevitable result of the agency's ability to enforce broad reasonableness standards and have proposed expanding its role.[174] Thus, the FTC's function remains a source of debate and exemplifies the uncertainty surrounding enforcement in the cybersecurity realm.

III. PROACTIVE SOLUTIONS FOR PROTECTING CONSUMERS

Given the inevitable rise of data breaches, consumer information will remain vulnerable unless drastic changes are made to influence how companies collect and store data. Private litigation has provided little incentive for companies to make these necessary changes.[175] Instead, a robust national data security law must be adopted to prevent consumer information from being exposed by data breaches. First, this should be modeled on current federal privacy laws like HIPAA or

168. *LifeLock to Pay $100 Million to Consumers to Settle FTC Charges It Violated 2010 Order*, FED. TRADE COMM'N (Dec. 17, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated [https://perma.cc/BD2C-9RLQ].

169. *Id.*

170. *Id.*

171. *Id.*

172. *See Operators of AshleyMadison.com Settle FTC, State Charges Resulting from 2015 Data Breach that Exposed 36 Million Users' Profile Information*, FED. TRADE COMM'N (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting [https://perma.cc/7NUL-EXHJ] (announcing the FTC's settlement with Ashley Madison for deceiving customers and releasing 36 million users' accounts).

173. Hartzog & Solove, *supra* note 31, at 2232.

174. *Id.* at 2259–63.

175. *See supra* Part II.A.

GLBA, as well as state data protection legislation. Ideally, this new law would extend to all companies using consumers' personal information and would create minimum-security requirements for collecting and storing this information. Additionally, it should expand the jurisdiction of the FTC as the primary enforcement agency for data breach claims. Second, since even companies with strong security practices will inevitably face cyber threats, similarly proactive solutions must be implemented on the front-end to minimize the exposure of personal information. Regulating the use of SSNs or creating a decentralized identification system, for example based on blockchain technology, are potential solutions for protecting this information.

A. Implementing a National Data Security Law

A national data security law is a necessary preventive measure for data protection for three reasons. First, legislation would be more efficient than relying primarily on private litigation to encourage cybersecurity reforms on a company-by-company basis. Second, a federal law would create uniform standards for companies' data collection, storage, and usage, instead of depending on a patchwork of state laws. Third, from an enforcement perspective, increasing the power of the FTC would encourage necessary compliance with the new law.

First, the challenges associated with private litigation make it an inefficient route for protecting consumers. While plaintiffs have continued to propose novel claims following data breaches, the legal landscape has failed to move in tandem with technological advances.[176] Litigants are forced to work within existing legal structures ill-suited for responding to data breaches and the unique injuries that follow.[177] Some argue that new data statutes should create a private right of action.[178] This would make it easier to support a claim of injury after data breaches. While the constitutionality of this solution would be at

176. *See* Dowty *supra* note 22, at 687 ("In the realm of data breaches, technology is progressing rapidly; consequently, there is a lag time between the progress of technology and progress of the law."); *see also supra* note 84 (detailing data breach litigation trends in 2017 and the procedural status of various cases, such as Yahoo).

177. *See supra* Part III.A.

178. *See, e.g.*, Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How To Fix It*, 42 J. CORP. L. 461, 472 (2016) (arguing that a private right of action would facilitate plaintiffs' ability to show concrete harm without accompanying damages).

issue,[179] even a successful statutory private right of action would be a reactionary solution. Besides the potential costs of litigation and bad press, companies unaffected by data breaches have little incentive to alter their data collection, usage, and storage procedures. Many boards of directors and executives may realize the potential threat of cyberthreats in theory but overlook this possibility within their own companies. Legislation is needed to encourage changes in the security context. Otherwise, these perceived risks will continue to be discounted. Data security has become such a pressing issue that we can no longer trust boards to make decisions surrounding consumer data without a new legislative oversight framework.

Second, a national law would provide a uniform, and potentially more robust, solution than the existing collection of state laws. Currently, most state laws require companies to notify customers after their personal information has been stolen.[180] However, many of these state laws fail to set demanding cybersecurity standards and limit the definition of what constitutes personal information.[181] In contrast, setting a high bar for data security through a national law would be extremely advantageous from an efficiency perspective by providing a unified standard. Companies whose operations typically transcend state and even national boundaries, would not need to navigate multiple states' divergent security and breach notification laws.

Critics of national data laws may point to the interaction between federal and state environmental policy, arguing that statutes like California's Consumer Privacy Act of 2018 will be effective mechanisms for privacy protection across the entire country. However, it remains to be seen whether this Act will have its intended effect, because other states may create their own competing data privacy laws or legislate ways to allow companies to avoid the Act's requirements in their state. While it may be more cost-effective for car manufacturers to set uniform motor vehicle air emissions standards based on stringent California laws, technology allows companies the flexibility to be more

179. *See* Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992) (finding that plaintiffs failed to establish Article III standing although the Endangered Species Act created a right of action). *But see* Patrick J. Lorio*, Access Denied: Data Breach Litigation, Article III Standing, and A Proposed Statutory Solution*, 51 COLUM. J.L. & SOC. PROBS. 79, 116 (2017) (arguing that a "data breach statute . . . need only give the right to sue to those specific individuals whose personal information is exposed" to circumvent concerns stemming from *Lujan*).

180. *See supra* note 30 and accompanying text.

181. *See supra* notes 144–47 and accompanying text (examining the divergent requirements and breadth of states' existing data security and breach laws).

discerning about whose information they collect. For example, company X based in New York may have no trouble filtering out which of their customers are from California and which are from other states. So, even if states like California still opted for even more robust standards, a national law would set a baseline for company X's use of the average customer's data, while allowing the company to be more restrictive with the California customer's data. Such a bifurcated system is not inconceivable because companies already collect as much information as possible on consumers, and have little incentive to stop unless nudged by increased regulation.

This proposal has precedent, as national laws for protecting medical and financial information—HIPAA and GLBA—already exist. A new nationwide data law could be built using these existing frameworks. As in Massachusetts, broadening the definition of "personal information" should expand the universe of companies subjected to the new law.[182] Similarly, on the technical side, this law should create minimum cybersecurity standards for data storage, require encryption of all forms of PII, and mandate adequate security training for all companies. The U.S. Department of Commerce's National Institute of Standards and Technology has already proposed technical guidelines for federal agencies using digital identification mechanisms.[183] Similar guidelines should be used to set industry standards based on companies' size and existing technological infrastructure. Additionally, as in New York, a new law should require companies of certain sizes to add a Chief Information Security Officer position and ensure they sign off on cybersecurity compliance.[184] From the rights perspective, the California Consumer Privacy Act of 2018 provides an excellent starting point for giving consumers access to their information.[185] However, more can be accomplished, including requiring companies to gain opt-in consent prior to collecting this data.[186]

---

182. *See supra* note 155 and accompanying text (applying the state's security regulation to "[e]very person that owns or licenses personal information about a resident of the Commonwealth").

183. PAUL A. GRASSI, MICHAEL E. GARCIA & JAMES L. FENTON, U.S. DEP'T OF COMMERCE, NIST SP 800-63-3, DIGITAL IDENTITY GUIDELINES (2017).

184. *See supra* notes 157–60 and accompanying text.

185. *See supra* notes 150–53 and accompanying text.

186. Adam Schwartz, Lee Tien & Corynne McSherry, *How to Improve the California Consumer Privacy Act of 2018*, Electronic Frontier Foundation (Aug. 8, 2018), https://www.eff.org/deeplinks/2018/08/how-improve-california-consumer-privacy-act-2018 [https://perma.cc/X26V-R6XG].

Additionally, while efforts to enact national data security laws have failed in the past, after large-scale scandals, like Equifax or Facebook, increased public conversations may lead to new regulatory actions.[187] The Sarbanes-Oxley Act was enacted in the wake of numerous corporate accounting scandals between 2000 and 2002, like Enron and Arthur Andersen.[188] And lawmakers in Congress are already pushing for increased cybersecurity regulations.[189] One example, the Personal Data Notification and Protection Act, would require companies to disclose breaches within thirty days to the FTC and Department of Homeland Security.[190] Another is the Data Broker Accountability and Transparency Act, which would allow the public to opt-out of having personal data collected and sold by brokers.[191] The EU's General Data Protection Regulation ("GDPR"), which went into effect in May 2018, exemplifies what a far-reaching privacy law looks like.[192] The GDPR adopts standards for utilizing EU citizens' data, including requiring explicit consent for using consumers' information and allowing consumers to access copies of their data or delete it completely.[193] At first glance, implementing these regulations may

187. Jeff John Roberts, *Why Equifax Executives Will Get Away with the Worst Data Breach in History*, FORTUNE (Sept. 16, 2017), http://fortune.com/2017/09/16/equifax-legal/ [https://perma.cc/9JW4-Z88U] (citing Duke University School of Law Professor Sam Buell's argument that Equifax may trigger new regulatory oversight).

188. Rosemary Peavler, *The Enron Scandal that Prompted the Sarbanes-Oxley Act*, BALANCE (July 16, 2017), https://www.thebalance.com/sarbanes-oxley-act-and-the-enron-scandal-393497 [https://perma.cc/YB8J-RS7V].

189. Christopher Mims, *After Equifax, Should the Government Force Companies To Report Hacks?*, WALL ST. J. (Sept. 24, 2017, 8:00 AM), https://www.wsj.com/articles/should-the-u-s-require-companies-to-report-breaches-1506254402 [https://perma.cc/G7UX-AVUK].

190. *Id.*

191. Joe Uchill, *Dems Propose Data Security Bill After Equifax Hack*, HILL (Sept. 4, 2017, 1:54 PM), http://thehill.com/policy/cybersecurity/350694-on-heels-of-equifax-breach-dems-propose-data-broker-privacy-and-security [https://perma.cc/4SAZ-V6WE].

192. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Council Directive 95/46/EC, 2016 O.J. (L 119) 1. For a full background on the GDPR, as well a user-friendly FAQ, see *2018 Reform of EU Data Protection Rules*, EUROPEAN COMMISSION (2018), https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en [https://perma.cc/3CKV-V8KV].

193. *See* Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would Be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-u-s/5b07038b1b326b492dd07e83/?utm_term=.806cce7e6167 [https://perma.cc/BPX8-VVX6]

appear improbable in the U.S., but the "public appetite for data privacy regulation" is only increasing.[194]

Third, since there is already widespread discussion of the FTC in the data breach context,[195] a new data security law should clarify and expand the agency's role. Increasing the FTC's power will provide a viable enforcement mechanism for encouraging compliance with any new national standards. The FTC should be able to impose heightened civil penalties on companies failing to implement reasonable protections in accordance with these regulations.[196] Additionally, since the FTC is required to provide fair notice to the entities it regulates,[197] creating a national data security law would help tie this notice to a uniform industry standard. Giving the FTC explicit rulemaking authority would also allow it to "develop more systematic rules where they are needed."[198] At bottom, companies would be more likely to comply with new federal legislation if the role of enforcement agencies like the FTC was clearly defined and tougher penalties could be levied for violations.

A new data security law may finally begin to take shape in the next few years because of the rapid increase in data breaches and the heightened publicity surrounding their aftermath.[199] Lobbyists for data brokers, as well as political hurdles in Congress—obstacles arising in

(examining the differences between the U.S. and the EU's privacy regimes in the wake of the GDPR legislation).

194. *Id.*

195. *E.g.*, Hartzog & Solove, *supra* note 31; Arias, *supra* note 129; *see also* Corey L. Andrews, *Federal Court's Embrace of FTC Data-Breach Settlements as 'Common Law' Treads on Due Process*, FORBES (Dec. 19, 2017, 11:51 AM), https://www.forbes.com/sites/wlf/2017/12/19/ federal-courts-embrace-of-ftc-data-breach-settlements-as-common-law-treads-on-due-process/ #244ed50e24d1 [https://perma.cc/Q9PH-C6W3] (arguing against the FTC's recent use of "enforcement actions (and the resulting consent decrees) as a source of 'common law' that places the business community on sufficient notice of what data-security practices § 5 of the FTC Act requires").

196. *Cf.* Arias, *supra* note 129 (noting that "since 2001, the FTC has settled some 60 cases against companies the FTC alleges failed to provide reasonable protections for consumers' personal information").

197. Hartzog & Solove, *supra* note 31, at 2291.

198. *Id.* at 2299.

199. In November 2017, Senators Bill Nelson, Richard Blumenthal, and Tammy Baldwin introduced a federal data breach notification bill that would require companies to report data breaches within 30 days or face criminal consequences. Selena Larson, *Senators Introduce Data Breach Disclosure Bill*, CNN TECH (Dec. 1, 2017, 10:51 AM), https://money.cnn.com/2017/12/01/technology/bill-data-breach-laws/index.html [https://perma.cc /9QR8-B6MK]. While it is a strong start, the bill does not go far enough to set mandatory cybersecurity standards for protecting consumers' information pre-data breach.

tandem with any large-scale legislation—may delay this process. Nevertheless, because of the increasing privacy concerns, data security and breaches are trending from niche topics into regularly-debated bipartisan issues.[200]

B. Social Security Numbers and Blockchain Technology

While federal legislation is necessary for setting uniform security standards, this alone is unlikely to prevent companies from continuing to collect and sell consumers' personal and financial information. Proactive solutions must also address the inputs in this equation by going to the source—individuals and companies' universal reliance on outdated forms of PII. One viable option is to incorporate a provision in this proposed national data security law that curtails companies' liberal use of Social Security numbers. A second, more long-term goal is to create an alternative identification system altogether; for example, a decentralized identification system based on distributed ledger technology like blockchain.

1. *Regulation of Social Security Numbers*. New regulations in federal law should incorporate provisions to limit companies' use of Social Security numbers in the private sector. SSNs were not intended to be personal identifiers.[201] Without federal regulations, banks, hospitals, government agencies and companies alike have turned SSNs into an easy method of identifying and authenticating people and their information.[202] However, once these identifiers are compromised in a data breach, they are almost impossible to change, unlike a standard password.[203]

One solution is for Congress to explicitly prohibit companies from using SSNs as passwords and personal identifiers.[204] This would require the private sector to develop alternate means of identifying consumers. For example, companies could assign each customer a company-specific ID. If a healthcare company was breached and exposed its customer data, but didn't possess SSNs, it would be harder for identity

200. *See supra* note 10 and accompanying text.

201. Puckett, *supra* note 44, at 67.

202. Daniel Castro, *Time to Retire Social Security Numbers*, REAL CLEAR POL'Y (Sept. 16, 2017), http://www.realclearpolicy.com/articles/2017/09/16/time_to_retire_social_security_numbers_110358.html [https://perma.cc/AGA2-ZXFE].

203. *Id.*

204. *Id.*; *see* Darrow & Lichtenstein, *supra* note 55, at 54 (arguing for a federal law prohibiting the use of SSNs as passwords).

thieves to link this information to customers' accounts at different companies. This reduces the potential of hackers exploiting SSNs as a "key." Although potentially ameliorating security concerns, this prohibition also shifts the burden to individuals. It requires consumers to maintain and protect their own company-specific IDs. Thus, any prohibition on SSNs must result from a weighing of the security improvement with the added inefficiencies that result from using multiple identifiers.

Instead, the government should begin phasing out the Social Security number altogether. In 2007, the Office of Management and Budget issued a memo requiring federal departments and agencies to begin eliminating the unnecessary use of SSNs.[205] The House Ways and Means Committee is exploring this option and has discussed having agencies, such as the Centers for Medicare & Medicaid Services, eliminate the use of beneficiaries' SSNs as a primary identifier on their Medicare cards.[206] Individual states, like California, have been at the forefront of these changes by limiting the printing of SSNs on IDs and certain membership cards.[207]

If the U.S. government eliminates its own reliance on Social Security numbers, private companies are likely to follow suit. SSNs are widely distributed across companies in part because consumers have been conditioned to readily hand over these numbers.[208] If the federal government and states started phasing out their usage, it would change how individuals view their SSNs. Alternatively, if the number was solely used for Social Security benefits, there would be no reason to collect SSNs outside of the employment context. Individuals would be warier of habitually providing this information since companies would have no specific use for the number.

---

205. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, OMB MEM. NO. 07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION 7 (2007).

206. *Federal Agencies Have "A Long Way to Go" to Limit the Use of Social Security Numbers and Adequately Protect Americans' Identities*, U.S. HOUSE REPRESENTATIVES COMMITTEE WAYS & MEANS: BLOG (May 23, 2017), https://waysandmeans.house.gov/federal-agencies-long-way-go-limit-use-social-security-numbers-adequately-protect-americans-identities/ [https://perma.cc/TYJ8-C2B6].

207. FED. TRADE. COMM'N, SECURITY IN NUMBERS: SSNS AND ID THEFT 8 (2008), https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf [https://perma.cc/8KDT-G7KZ].

208. *Cf. supra* note 52 and accompanying text (listing the many businesses that obtain consumers' SSNs).

Companies that persistently request Social Security numbers could even be at a financial disadvantage. If this information was stolen in a data breach, hackers may have a better chance of successfully conducting identity theft. This would result in increased litigation against companies by victims of data breach and identity theft. Accordingly, minimizing the ubiquity of SSNs in daily life may create a disincentive for companies to collect this personal information in the first place.

2. *Blockchain-Based Personal Identification Systems*. In the long-term, legislators should explore alternative identification systems and methods for storing personal information that would make Social Security numbers obsolete. Biometric identification systems have been proposed,[209] but must confront significant technological[210] and legal challenges.[211] A new national ID card is another possibility, but faces similar concerns.[212] Though still a fledgling technology, blockchain appears to be one of the most promising options because of its unique security properties.

At its simplest, blockchain is an example of a distributed ledger system.[213] This system is like a "giant, global spreadsheet that runs on millions and millions of computers. It's distributed. It's open source, meaning that anyone can view and change the underlying code. It's

209. "Biometrics is '[t]he science of automatic identification or identity verification of individuals using physiological or behavioral characteristics.'" Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1477 n.3 (2013) (quoting JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007)). Biometric data includes individuals' digital photos, fingerprints and iris scans, and DNA. *Id.* at 1478. The theory is that this information is unique to every person and would be much harder than Social Security numbers to easily duplicate. *Id.* at 1477–78.

210. *See, e.g.*, Aditi Roy, Nasir Memon & Arun Ross, *MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems*, 12 IEEE TRANSACTIONS ON INFO. FORENSICS & SEC. 2013, 2013 (2017) (arguing that certain fingerprint-based authentication systems, like on smartphones, may be vulnerable to impersonations).

211. The main apprehensions stem from Fourth Amendment privacy concerns over the government's control of individuals' personal information and the potential for misuse through increased cybersurveillance. *See* Hu, *supra* note 209, at 1481–82 (arguing that "it is necessary to consider what role, if any, the Fourth Amendment will play in restraining a rapidly evolving bureaucratized cybersurveillance movement").

212. *See 5 Problems with National ID Cards*, ACLU, https://www.aclu.org/other/5-problems-national-id-cards [https://perma.cc/w7F5-788M] (highlighting how national ID cards create vexing technical challenges and menacing legal problems).

213. *See* Nolan Bauerle, *What is a Distributed Ledger?*, COINDESK, https://www.coindesk.com/information/what-is-a-distributed-ledger/ [https://perma.cc/X2SB-RQG6] ("In its simplest form, a distributed ledger is a database held and updated independently by each participant (or node) in a large network.").

truly peer to peer; it doesn't require powerful intermediaries to authenticate or to settle transactions."[214] For example, the Bitcoin blockchain anonymously keeps track of financial transactions between individuals using Bitcoin currency.[215] Instead of financial transactions, a blockchain system could record any structured information from land ownership to marriage records.[216] Blockchain is open-source and public, but the information it records can be encrypted.[217] So, someone may be able to view the entire encrypted database without being able to read its contents.[218]

In the public sector, encrypted distributed ledgers have a number of uses. Such ledgers could be used to keep "certified copies of identity documents, biometric test results, health data, or academic and training certificates online, available at all times."[219] To tie this information to individuals, each person would receive a unique code called a "blockchain hash" that would be imprinted on every digital transaction as a personal identifier.[220] While similar to a SSN in that consumers would be required to keep their blockchain hash as a sort of key,[221] this information could be readily accessible and controlled by individuals.[222] In contrast, most personal information, like SSNs, is

214. Don Tapscott, *How Blockchains Could Change the World*, MCKINSEY & CO. (May 2016), https://www.mckinsey.com/industries/high-tech/our-insights/how-blockchains-could-change-the-world [https://perma.cc/9SV6-UR6Z].

215. *See* Nathaniel Popper, *What Is Bitcoin? All About the Mysterious Digital Currency*, N.Y. TIMES (May 15, 2017), https://www.nytimes.com/2017/05/15/business/all-about-bitcoin-the-mysterious-digital-currency.html [https://perma.cc/QBH9-WVR3] (describing how the anonymous creation of a Bitcoin address allows a seller to accept Bitcoin payments).

216. Tapscott, *supra* note 214.

217. Michael Mainelli, *Blockchain Could Help Us Reclaim Control of Our Personal Data*, HARV. BUS. REV. (Oct. 5, 2017), https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data [https://perma.cc/75TL-XPNS].

218. *Id.*

219. *Id.*

220. Nafeesa Syeed & Elizabeth Dexheimer, *The White House and Equifax Agree: Social Security Numbers Should Go*, BLOOMBERG (Oct. 3, 2017), https://www.bloomberg.com/news/articles/ 2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go [https://perma.cc/45QZ-WYC5].

221. Syeed and Dexheimer described how such a system might work:

> [T]he government could issue each person a public key and private key. If people were to open a bank account, for instance, they could provide their public key—instead of a Social Security number—and the bank would send a message that could only be decrypted using their private key. If the private key gets compromised, the government could easily issue another one.

Id.

222. *See* Mainelli, *supra* note 217 (envisioning a system in which individuals would always control access to their personal valuable documents through a cryptographic key).

currently stored using large centralized systems. Once these systems are hacked, the entire database of information becomes available. Equifax suffered from this very problem.[223] The switch to blockchain technology makes the distributed ledger system arguably safer because hackers would have to target and decode each individual encrypted ledger to access the contents of this information.[224]

Estonia provides an instructive example. For several years, the government of Estonia has been using a similar distributed ledger system called e-Estonia.[225] Every citizen in Estonia has a nationally-issued Estonia ID card for keeping track of public, financial, medical and emergency services, as well as driving, paying taxes online, and e-voting.[226] Instead of keeping a national ID number or driver's license number in a centralized database, the Estonia ID card uses a blockchain-like distributed ledger system.[227] This gives individuals greater control over their personal information and allows them to access their encrypted data electronically.[228]

In the U.S., several states have embraced blockchain technology. For example, recently, "legislators amended Arizona's Electronic Transactions Act (the AETA) to clarify that 'electronic records, electronic signatures, and smart contract terms secured through blockchain technology and governed under UCC Articles 2, 2A and 7 will be considered to be in an electronic form and to be an electronic signature under AETA.'"[229] Nevada and Vermont have passed similar

223. *See* Seth Fiegerman, *Why the Equifax Breach Makes You Feel So Helpless*, CNN (Sept. 8, 2017, 1:25 PM), https://money.cnn.com/2017/09/08/technology/business/equifax-breach-helpless/index.html [https://perma.cc/6HLH-MVZV] (recognizing Virginia Senator Mark Warner's comment that Congress "needs to rethink data protection policies, so that enterprises such as Equifax have fewer incentives to collect large, centralized sets of highly sensitive data").

224. *Id. But see* Raja Raman & Mahesh Mangnaik, *Blockchain Can Transform the World, But Is It Fool-Proof?*, HUFFINGTON POST: INDIA (Jan. 23, 2017), http://www.huffingtonpost.in/raja-raman/blockchain-can-transform-the-world-but-is-it-fool-proof_a_21660586/ [https://perma.cc/HZE5-427W] (arguing that software risks remain and individuals' keys may still be stolen).

225. Joyce Shen, *e-Estonia: The Power and Potential of Digital Identity*, THOMSON REUTERS: ANSWERS ON (Dec. 20, 2016), https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital-identity/ [https://perma.cc/AUZ3-8MC2].

226. *Id.*

227. *Id.*

228. Vivienne Walt, *Is This Tiny European Nation a Preview of Our Tech*, FORTUNE (Apr. 27, 2017), http://fortune.com/2017/04/27/estonia-digital-life-tech-startups/ [https://perma.cc/7MMV-TVSG] ("[F]or example, Finns and Estonians can visit doctors in the other country and automatically call up their medical records—all stored online.").

229. Riley T. Svikhart, *Blockchain's Big Hurdle*, 70 STAN. L. REV. ONLINE 100, 103 (2017) (quoting Jeffrey Neuburger, *Arizona Passes Groundbreaking Blockchain and Smart Contract Law–State Blockchain Laws on the Rise*, PROSKAUER: NEW MEDIA & TECH. L. BLOG

amendments,[230] and a blockchain-based birth registry and ID system is currently being considered in Illinois.[231] The Illinois Blockchain Initiative would create a "self-sovereign" identity for Illinois citizens on a distributed ledger.[232] It would store government-verified attributes, such as legal name, date of birth, sex, and blood type, for each person at birth.[233] The result is that "[b]usinesses and governments will be able to verify and authenticate citizens by requesting encrypted access to [their electronically stored information]. This minimizes the need for entities to establish, maintain, and rely upon their own proprietary databases of identity information."[234] Across the U.S., such an initiative, like the one in Illinois, would be unprecedented.

New mechanisms for storing personal information would enable individuals to constantly access and monitor this data. As in Estonia, such changes would better facilitate citizens efficient interactions with the state, as well as companies that requested consumer information. In addition, by enabling consumers to decide when to release their information to these companies, citizens would be able to track how their data was used. And, following the Equifax breach, legislators have proposed giving consumers the opportunity to opt-out of the credit reporting industry.[235] This parallels the conversation surrounding the adoption of blockchain technology. Both concepts seek to put consumers back in control of their own information.

A blockchain-based system does face legal and infrastructure challenges. Like biometrics, blockchain is tied into the larger legal issue of identity management.[236] Individuals must willingly provide personal

---

(Apr. 20, 2017), http://newmedialaw.proskauer.com/2017/04/20/arizona-passes-groundbreaking-blockchain-and-smart-contract-law-state-blockchain-laws-on-the-rise/ [https://perma.cc/FHR8-JTD2]).

230. *Id.*

231. *See* Mainelli, *supra* note 217 (pointing out that Illinois is testing a blockchain-based birth registry/ID system).

232. *Illinois Partners with Evernym to Launch Birth Registration Pilot*, ILL. BLOCKCHAIN INITIATIVE (Aug. 31, 2017), https://illinoisblockchain.tech/illinois-partners-with-evernym-to-launch-birth-registration-pilot-f2668664f67c [https://perma.cc/9KV4-7E53].

233. *Id.*

234. *Id.*

235. Uchill, *supra* note 191.

236. Identity management "involves two fundamental processes[,]" identification and authentication. Thomas J. Smedinghoff, *Solving the Legal Challenges in Verifying Online Identity*, 8 SCITECH L. 10, 11 (2011). Identification is "the process of verifying certain identity attributes about a person and issuing an identity credential to reflect those attributes." Authentication is "the process of later verifying that a particular person presenting that credential and claiming to be that previously identified person is, in fact, such person." *Id.*

information to identity providers, like governments, and trust them to better utilize this information through blockchain rather than through the existing system. In the U.S., the government would be required to play a major role in devising, storing, and monitoring this new blockchain-based system. There may be an initial backlash from consumers because of potential privacy questions. While the U.S. maintains less stringent privacy regulations than places like the EU,[237] there is a strong legal tradition of upholding privacy rights.[238] Even if proposals like the Illinois Blockchain Initiative are successfully implemented for newborns, any new identity system based on blockchain will likely face an uphill legal battle from the rest of society.[239]

Scaling this project across the U.S. would also face significant hurdles. Estonia is a small nation with a population of just 1.3 million.[240] Unlike the U.S.' mix of federal and state laws developed over hundreds of years, Estonia had the opportunity to rebuild its entire identity infrastructure after the fall of the U.S.S.R.[241] This meant that Estonia could utilize the latest digital technology in all facets of society—from creating reliable identification systems to providing free Wi-Fi as a basic human right.[242]

While not an insignificant transition, the prospect of altering the Social Security number system has been gaining traction since the Equifax breach. During former Equifax CEO Richard Smith's testimony before Congress, he said, "What is a better way to identify consumers in our country in a very secure way? I think that way is something different than an SSN, a date of birth and a name."[243] These statements have been echoed by the Trump administration, which has called on federal departments and agencies to consider replacing the existing system.[244] The reality is that Social Security numbers have become an antiquated means of personal identification and a new reliable method of identification is a matter of profound necessity.

---

237. *See supra* notes 192–94 and accompanying text for a brief introduction to the GDPR.

238. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (making a seminal argument about the American tradition of privacy).

239. *See, e.g.*, Tom Kulik, *Why Blockchain And The GDPR Collide Over Your Personal Data*, ABOVE THE LAW (Oct. 8, 2018), https://bit.ly/2EHRAL9 [https://perma.cc/AJG3-GSPF].

240. Walt, *supra* note 228.

241. *Id.*

242. *Id.*

243. Syeed & Dexheimer, *supra* note 220.

244. *Id.*

CONCLUSION

"Data breach" has become a common phrase in the American public's lexicon. And for good reason—breaches are increasing not only in frequency, but also in scale, with the potential to adversely affect every U.S. citizen. Consumers and shareholders of companies will likely continue filing lawsuits in response to these breaches. Some may succeed based on novel legal theories and relentless class-action lawsuits.[245] Yet, many will flounder at the initial standing and pleading stages.[246] While states like California, New York, and Massachusetts are at the forefront of strengthening state-specific data privacy laws, a unified federal law on the scale of the EU's GDPR is a better alternative than the existing patchwork.

Accordingly, Congress must pass a comprehensive piece of data privacy legislation. A national data law is a better alternative to the existing patchwork of state laws and will help set minimum security standards for collecting, storing, and using consumers' data. The U.S. government has the infrastructure to create a proactive public solution, like HIPAA and GLBA. If the FTC's cybersecurity powers are simultaneously expanded, the agency would help implement, regulate, and enforce this legislation.

Additionally, as the national conversation shifts to concerns regarding personal identity and restoring consumers' control over their data, phasing out SSNs is one example of an attainable solution. Another option is reexamining the concept of PII altogether. The Illinois Blockchain Initiative hints at the future of secure and reliable personal information storage using a blockchain-based system.[247] As of publication, blockchain appears to be the solution du jour for many intractable technological issues. Regardless of blockchain's longevity, it is undeniable that the currently employed system in the U.S based on a rudimentary nine-digit pin code is inherently flawed and unsustainable. These solutions are thus designed to provide potential alternatives and help reframe our collective understanding of PII. Now, it is up to legislators and citizens to demand that these essential changes come to fruition.

245. *See supra* notes 68 & 122 and accompanying text.

246. *See supra* notes 69, 73, 87 and accompanying text.

247. *See supra* note 232 and accompanying text.